IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JULIA A. HARRIS, individually and on behalf of all others similarly situated, Plaintiff, v. HUDSON'S BAY COMPANY, SAKS FIFTH AVENUE LLC, and LORD & TAYLOR LLC, Defendants.	Civil Action No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Julia A. Harris ("Plaintiff"), individually and on behalf of the class ("Class") and subclass ("Sub-Class") defined below, alleges the following against Hudson's Bay Company ("HBC" or the "Company"), Saks Fifth Avenue LLC ("Saks"), and Lord & Taylor LLC ("Lord & Taylor"), together with HBC and Saks, the ("Defendants"), based upon personal knowledge with respect to herself and on information and belief derived from, among other things, the investigation of counsel and a review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiff brings this class action case against HBC, and its agents and wholly owned subsidiaries, Saks and Lord & Taylor, in connection with a massive data breach (the "Data Breach") which occurred at some point commencing in May 2017 and continued until about April 2, 2018.

2. Specifically, at some point commencing in May 2017, Hudson's computer systems were hacked by a criminal group called JokerStash. Hudson, however, was unaware both that its systems were vulnerable and that it had been hacked.

3. In the meantime, hackers obtained the personal identification information or PII of over 5,000,000 customers of Hudson's wholly owned subsidiaries, Saks and Lord & Taylor, making it one of the largest payment card data breaches that has occurred.

4. That information included customer credit card and other information sufficient for the hackers to make fraudulent charges on customers' accounts, among other damage.

5. Hudson, however, was so unaware of the vulnerability of its data systems that it did not even learn of the Data Breach until it read a blog by a New York based cyber security firm called Gemini Advisory ("Gemini"), disclosing that both Saks and Lord & Taylor had been breached.

6. HBC could have prevented the Data Breach. Instead, HBC disregarded the rights of Plaintiff and Class and/or Sub-class members by failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard their PII, failing to take available steps to prevent and stop the breach from happening, and failing to monitor and detect the breach on a timely basis.

7. As a result of the Data Breach, the PII of the Plaintiff and Class and/or Sub-class members have been exposed to criminals for misuse, and are now being disseminated on the dark web. The injuries suffered by Plaintiffs and Class and/or Sub-class members, as a direct result of the Data Breach include:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, the costs of purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused through the sale of Plaintiff's and Class and/or Sub-class members' information on the dark web or elsewhere;

h. damages to and diminution in value of their PII entrusted to HBC for the sole purpose of purchasing products and services from HBC; and

i. the loss of Plaintiff's and Class and/or Sub-class members' privacy.

8. The injuries to the Plaintiff and Class and/or Sub-class members were directly and proximately caused by the failure of HBC, and its agents, Saks and Lord & Taylor to implement or maintain adequate data security measures for PII.

9. Further, Plaintiff retains a significant interest in ensuring that her PII, which, while stolen, remains in the possession of HBC and/or Saks or Lord & Taylor, is protected from further

breaches, and seeks to remedy the harms she has suffered on behalf of herself and similarly situated consumers whose PII was stolen as a result of the Data Breach.

10. Plaintiff brings this action to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach, and is presently being released by JokerStash on the dark web. Plaintiff seeks the following remedies, among others: statutory damages under state laws, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring HBC and/or its agents, Saks and Lord & Taylor, to implement improved data security measures.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000 exclusive of interest and costs. Plaintiff and the Defendants are citizens of different states, or a foreign country. There are more than 100 putative class members.

12. This Court has personal jurisdiction over HBC because it regularly conducts business in New York, has availed itself of both the law of New York State and the United States, and thus has sufficient minimum contacts with New York and the United States such that the exercise of jurisdiction over it is consistent with principles of due process. This Court has jurisdiction over Saks and Lord & Taylor because they both maintain their principal places of business in New York and are thus resident here.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because HBC maintains offices in this District, as do Saks and Lord & Taylor. *See* (https://www3.hbc.com/press-release-container/hudsons-bay-company-to-open-saks-fifth-

avenue-and-saks-off-5th-stores-in-lower-manhattan-combine-nyc-office-locations/). Moreover, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

Plaintiff

14. Plaintiff is a resident of Connecticut. She shopped at Lord & Taylor in Connecticut and New York during the period of compromise and paid with a credit card, thus giving her PII to HB and Lord & Taylor.

Defendants

15. Defendant HBC is a Canadian corporation amalgamated under the Canada Business Corporations Act and domiciled in Canada. The Company owns and operates department stores in Canada and the United States under Hudson's Bay, Lord & Taylor, Saks Fifth Avenue, Saks Fifth Avenue OFF 5TH, Find @ Lord & Taylor, Gilt and Home Outfitters banners. Saks and Lord & Taylor are its wholly owned subsidiaries and act as its agents in the United States. HBC has control over both Saks and Lord & Taylor.

16. Defendant Saks is a Massachusetts limited liability company which is registered in New York State and maintains its principal place of business at 12 EAST 49th Street, New York, NY 10017, among other locations. Saks is an agent of Hudson.

17. Defendant Lord & Taylor LLC ("Lord & Taylor") is a Delaware Domestic Limited Liability Company which is registered in New York State and maintains offices in this District, among other locations. Lord & Taylor is an agent of Hudson.

BACKGROUND

18. On April 1, 2011, Gemini broke the news of the ("Data Breach) that Saks and Lord & Taylor had suffered a significant data breach[1]

19. On April 1, 2018, Gemini reported in significant part:

> On March 28, 2018, a notorious hacking JokerStash syndicate, also known as Fin7, announced the latest breach of yet another major corporation, with more than five million stolen payment cards offered for sale on the dark web. Several large financial institutions have confirmed that all tested records had been used before at Saks Fifth Avenue, Saks Fifth Avenue OFF 5TH, a discounted offset brand of luxury Saks Fifth Avenue stores, as well as Lord & Taylor stores.
>
> Although at this moment it is close to impossible to ascertain the exact window of compromise, the preliminary analysis suggests that criminals were siphoning the information between May 2017 to present. Based on the analysis of the available data, the entire network of Lord & Taylor and 83 Saks Fifth Avenue locations have been compromised. The majority of stolen credit cards were obtained from New York and New Jersey locations.
>
> With the declared number of compromised payment cards being in excess of five million, the current hacking attack is amongst the biggest and most damaging to ever hit retail companies. . . .
>
> * * * *
>
> Using our analytical tools, which were specifically developed in order to empower financial companies to monitor assets portfolio exposure within the deep & dark web, we have established with a high level of confidence that victims of the attack are Saks Fifth Avenue, Saks Fifth Avenue OFF 5TH, a discounted outlet of the luxury department store Saks Fifth Avenue, and Lord & Taylor Stores. Both companies are operated by Canadian retail business group Hudson's Bay Company (HBC). Despite the fact that HBC owns other retail brands, namely Galeria Kaufhof, and Home Outfitters, it appears that only Saks Fifth Avenue and Lord & Taylor were affected in this breach. The company also operates Gilt.com, a popular online shopping website.

[1] https://geminiadvisory.io/fin7-syndicate-hacks-saks-fifth-avenue-and-lord-taylor

20. Gemini further noted that the stolen PII was starting to be released on the "dark web", stating:

> As of this writing, only a minor part of compromised records have been offered for sale, with approximately 35,000 records for Saks Fifth Avenue and 90,000 records for Lord & Taylor.
>
> Considering the rather standard practice of marketplace operators in releasing stolen data gradually in order to avoid oversaturation of the market and to minimize the chances of identification of stolen records by the banks, it will take at least several months before the entire archive is offered for sale. For example, in the previous breach of Jason's Deli Restaurants in December of 2017, the JokerStash syndicate has announced that they stole five million payment cards; however, up until now, only approximately a quarter of all payment cards were released for sale.
>
> Despite the fact that the number of stolen records in both breaches is identical, the potential damage to cardholders could be significantly higher in the latest hacking attack. While diners at the affordable fast-food chain are less likely to purchase hi-end electronics like Apple computers and Microsoft Surface Books, which are coveted by cybercriminals for their high liquidity, it is also easier for banks to identify unusual shopping patterns and promptly block out-of-pattern transactions. However, cardholders who frequently shop at luxury retail chains like Saks Fifth Avenue are more likely to purchase high-ticket items regularly; therefore, it will be extremely difficult to distinguish fraudulent transactions from those of a legitimate nature, allowing criminals to abuse stolen payment cards and remain undetected for a longer period of time.

21. Also on April 1, 2018, ABC News reported that the breach had commenced over a year ago, stating that:

> There is evidence that the breach began about a year ago, said Dmitry Chorine, Gemini Advisory's co-founder and chief technology officer. He said the prolific hacking group has previously targeted major hotel and restaurant chains.
>
> The breach follows last year's high-profile hack of credit bureau Equifax that exposed the personal data of millions of Americans. This newest breach, however, more closely resembles past retail breaches that have targeted the point-of-sale systems used by companies from Home Depot to Target and Neiman Marcus.

> Chorine said the hackers' typical method is to send cleverly crafted phishing emails to company employees, especially managers, supervisors and other key decision-makers. Once an employee clicks on an attachment, which is often made to look like an invoice, the system gets infected.
>
> "For an entire year, criminals were able to sit on the network of Lord & Taylor and Saks and steal data," he said.
>
> Chorine said most of the stolen credit cards appear to have been obtained from stores in the New York City metropolitan area and other Northeast U.S. states. It's possible, he said, that those stores hadn't yet adopted the more secure credit card payment systems that have been rolled out elsewhere.

22. Plaintiff, and members of the Class and Sub-class have or will suffer actual injury as a direct result of HBC's data breach. In addition to fraudulent charges and damage to their credit, many victims spent or will spend substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

23. As a direct and proximate result of HBC's conduct, Plaintiff and the Class or Sub-class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

24. Plaintiff now has to take the time and effort to mitigate the actual and potential impact of the data breach on her everyday life, including placing "freezes" and "alerts" with credit reporting agencies, contacting her financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

25. Moreover, Plaintiff and the Class and/or Subclass have an interest in ensuring that their information, which remains in the possession of HBC, is protected from further breaches by the implementation of security measures and safeguards.

26. Plaintiff and the Class and/or Subclass have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including personal information and PCD;

b. Improper disclosure of their personal information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers' personal information and PII being placed in the hands of criminals and having been already misused via the sale of such information on the Internet black market;

d. Damages flowing from HBC's untimely and inadequate notification of the data breach;

e. Loss of privacy suffered as a result of the data breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

g. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market; and

h. The loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

CLASS ALLEGATIONS

27. Plaintiff brings this action as nationwide class under New York law on behalf of:

> All persons in the United States, whose personal information was compromised as result of the data breach first disclosed by HBC and others on April 1, 2018.

28. Alternatively, Plaintiff brings this action on behalf of a sub-class under Connecticut law on behalf of:

> All residents of Connecticut whose personal information was compromised as a result of the data breach first disclosed by HBC on April 1, 2018.

29. Excluded from each of the above Class or Sub-class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns.

30. The proposed Class or Subclass meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3):

31. **Numerosity.** The proposed Class and/or Sub-class include many thousands to millions of customers whose data was compromised in the Data Breach. While the precise number

of Class and/or Sub-class members has not yet been determined, the massive size of the Data Breach indicates that joinder of each member would be impracticable.

32. **Commonality.** Common questions of law and fact exist and predominate over any questions affecting only individual Class and/or Sub-Class members. The common questions include:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct constituted deceptive and unfair trade practices under the applicable consumer protection laws;

c. Whether Defendants had a legal duty to adequately protect Plaintiff's and Class and Sub-class members' personal information or PII;

d. Whether Defendants breached their legal duty by failing to adequately protect Plaintiff's and Class or Sub-class members' personal information;

e. Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and Class or Sub-class members;

f. Whether Defendants breached their duties to provide timely and accurate notice of the data breach to Plaintiff and Class and/or Sub-class members;

g. Whether and when Defendants knew or should have known that Plaintiff's and Class and/or Sub-class members' personal information stored on its computer systems was vulnerable to attack;

h. Whether Plaintiff and Class and/or Sub-class members are entitled to recover actual damages and/or statutory damages; and

i. Whether Plaintiff and Class and/or Sub-class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

33. **Typicality.** Plaintiff's claims are typical of the claims of the Class and/or Sub-class. Consumer Plaintiff and Class and Sub-class members were injured through Defendant's uniform misconduct and their legal claims arise from the same core Defendants' practices.

34. **Adequacy.** Plaintiff is an adequate representative of the proposed Class or Subclass as her interests do not conflict with the interests of the Class members she seeks to represent. Plaintiff's counsel is experienced in litigating consumer class actions and complex commercial disputes, and includes lawyers who have successfully prosecuted similarly massive retail data breach cases.

35. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against HBC. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

36. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Defendants acted or refused to act on grounds generally applicable to the Class or Sub-class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class or Sub-class as a whole.

37. Finally, all members of the purposed Class or Sub-class are readily ascertainable. Defendants have access to addresses and other contact information for millions of members of the Class or Sub-class, which can be used to identify Class or Sub-class members.

COUNT I

VIOLATIONS OF NEW YORK'S CONSUMER PROTECTION LAWS OR N.Y. GEN. BUS. LAW §§ 349 and 350 ON BEHALF OF A NATIONWIDE CLASS

38. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

39. Defendants' practices, acts, policies and courses of conduct, as described herein, including making representations that it possessed sufficient security to maintain the privacy of such PII, were intended to induce, and did induce, Plaintiff and the nationwide Class to provide their sensitive PII to Defendants.

40. Plaintiff and the nationwide Class, would not have provided their sensitive and personal PII if they had been told or knew that Defendants failed to maintain sufficient security to keep such PII from being hacked and taken by others, that Defendants failed to maintain the information in encrypted form, and that they failed for over a year to notice that their systems were vulnerable to hackers and in fact were being hacked during that time period.

41. Defendants practices, acts, policies and course of conduct are actionable in that:

a. Defendants actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the nationwide Class at the time they provided such PII information that Defendants did not have sufficient security or mechanisms to protect PII; and

b. Defendants failed to give adequate warnings and notices regarding the defects and problems with its security systems that it maintained to protect Plaintiff's and the nationwide Class's PII. Defendants possessed prior knowledge of the inherent defects in its IT

systems and failed to address the same or to give adequate and timely warnings that their systems were subject to and were being hacked, and that there had been a Data Breach.

42. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Defendants have, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system they maintained and failed to reveal the Data Breach timely and adequately.

43. Members of the public were deceived by and relied upon Defendants' affirmative misrepresentations and failures to disclose.

44. Such acts by Defendants are and were deceptive acts or practices which are and/or were, likely to mislead a reasonable consumer into providing his PII to Defendants. Said deceptive acts and practices are material. The requests for and use of such PII materials in New York by Lord & Taylor and Saks, who have principal places of business here, are controlled by New York law, and were consumer-oriented conduct that falls under the New York consumer fraud statutes, General Business Law §§ 349 and 350.

45. Defendants' wrongful conduct caused Plaintiff and the nationwide Class to suffer consumer-related injuries by causing them to incur substantial expense to protect them from the misuse of the PII materials by third parties and placing Plaintiff and the nationwide Class at serious risk for monetary damages.

46. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the nationwide Class seek statutory damages for each injury and violation which has occurred.

COUNT II

VIOLATIONS OF NEGLIGENCE ON BEHALF OF NATIONWIDE CLASS AND/OR THE SUB-CLASS

47. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

48. Defendants solicited, gathered, and stored personal information, including PII, of Plaintiff and the nationwide Class or, alternatively, the Sub-Class under Connecticut law to facilitate sales transactions.

49. Defendants knew, or should have known, of the risks inherent in collecting and storing the personal information of Plaintiff and the Class or Sub-class and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches by other national retailer and restaurant chains. Moreover, Defendants allowed their systems to be unprotected and subject to hacking for at least a year before they were on notice of the hacking which they first learned of from a third party, and were negligent in failing to notice or determine that their systems were vulnerable to attack.

50. Defendants owed duties of care to Plaintiff and the Class and/or Sub-class whose personal information was entrusted to it. Defendants' duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting personal information and PII in its possession;

b. To protect customers' personal information and PII using reasonable and adequate security procedures and systems that are compliant with the PCI-DSS standards and consistent with industry-standard practices;

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

d. To promptly notifying Plaintiff and Class or Sub-class members of the Data Breach.

51. Because Defendants knew that a breach of its systems would damage millions of its customers, including Plaintiff and Class or Sub-class members, it had a duty to adequately protect their personal information.

52. Defendants owed a duty of care not to subject Plaintiff and the Class or Sub-class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

53. Defendants knew, or should have known, that its computer systems were vulnerable to attack.

54. Defendants breached their duties of care by failing to provide for fair, reasonable and adequate safeguards of the personal information of Plaintiff and the Class or Sub-class, or adequate computer systems and data security practices to safeguard the personal information of Plaintiff and the Class and Sub-class.

55. Defendants breached their duties of care by failing to provide prompt notice of the data breach to the persons whose personal information was compromised.

56. Defendants acted with reckless disregard for the security of the personal information of Plaintiff and the Class and Sub-class because Defendants knew or should have known that its computer systems and data security practices were not adequate to safeguard the personal information that it collected and stored, which hackers were attempting to and did access for over a year.

57. Defendants acted with reckless disregard for the rights of Plaintiff and the Class or Sub-class by failing to provide prompt and adequate notice of the Data Breach so that they could

take measures to protect themselves from damages caused by the fraudulent use the personal information compromised in the data breach.

58. Defendants had a special relationship with Plaintiff and the Class and/or Sub-class. Plaintiff's and the Class or Sub-class' willingness to entrust Defendants with their personal information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the personal information that it stored on them) from attack.

59. Defendants' conduct also created a foreseeable risk of harm to Plaintiff and Class or Sub-class members and their personal information. Defendants' misconduct included failing to:

a. Secure its point-of-sale systems;

b. Secure access to its servers;

c. Comply with industry standard security practices;

d. Follow the PCI-DSS standards;

e. Encrypt PII at the point-of-sale and during transit;

f. Employ adequate network segmentation;

g. Implement adequate system and event monitoring;

h. Utilize modern payment systems that provided more security against intrusion;

i. Install updates and patches in a timely manner; and

j. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

60. Defendants also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and the Class' or Sub-class' personal information and promptly notify them about the data breach.

61. Defendants breached the duties it owed to Plaintiffs and Class or Sub-class members, as consumers, in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect their personal information both before and after learning of the data breach;

c. By failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the data breach; and

d. By failing to timely and accurately disclose that the personal information of Plaintiff and the Class or Sub-class had been improperly acquired or accessed.

62. But for Defendants' wrongful and negligent breach of the duties it owed Plaintiff and the Class or Sub-class members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

63. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class or Sub-class members have suffered damages.

64. The injury and harm that Plaintiff and Class or Sub-class, members, as consumers, suffered (as alleged above) was reasonably foreseeable.

65. The injury and harm that Plaintiff and Class or Sub-class members, as consumers, suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct.

66. Plaintiff and the Class or Sub-class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

NEGLIGENCE PER SE ON BEHALF OF THE NATIONWIDE CLASS, OR SUB-CLASS

67. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

68. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the personal information, including PII, of Plaintiff and the members of the Class or Sub-class.

69. The FTCA prohibits "unfair … practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect personal information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

70. Defendants solicited, gathered, and stored personal information, including PII, of Plaintiff and the Class or Sub-Class to facilitate sales transactions which affected commerce.

71. Defendants violated the FTCA by failing to use reasonable measures to protect personal information of Plaintiffs and the Class or Sub-class and not complying with applicable industry standards, as described herein.

72. Defendants' violation of the FTCA constitutes negligence *per se*.

73. Plaintiff and the Class or Sub-class are within the class of persons that the FTC Act was intended to protect.

74. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses,

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class or Sub-class.

75. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class or Sub-class have suffered, and continue to suffer, injuries and damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the data breach and/or false or fraudulent charges stemming from the data breach, including but not limited to late fees charges; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by contacting their financial institutions to place to dispute fraudulent charges, closing or modifying financial accounts, closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending.

76. Defendants either used the same computer systems and security practices in all states in which it maintains stores or negligently attempted to cut costs by exposing customer data in states where it did not feel obliged to follow best-practices.

77. Defendants breached their duties to Plaintiff and the Class or Sub-class by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class' or Sub-class' personal information.

78. Defendants' violation of the standards in the FTCA constitutes negligence *per se*.

COUNT IV

BREACH OF IMPLIED CONTRACT BY THE CLASS OR SUB-CLASS

79. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

80. When Plaintiff and the members of the Class or Sub-class, provided their personal information to Defendants in making purchases at either Saks or Lord & Taylor stores, they entered

into implied contracts by which Defendants agreed to protect their personal information and timely notify them in the event of a data breach.

81. Defendants invited its customers, including Plaintiff and the Class or Sub-class, to make purchases at its locations using payment cards in order to increase sales by making purchases more convenient.

82. An implicit part of the offer was that Defendants would safeguard the personal information using reasonable or industry-standard means and would timely notify Plaintiff and the Class or Sub-class in the event of a data breach.

83. HBC, in particular, also affirmatively represented that it would "continually review and enhance security" after a prior data leak.

84. Based on the implicit understanding and also on Defendants' representation, Plaintiff and the Class or Sub-class accepted the offers and provided Defendants with their personal information by using their payment cards in connection with purchases at HBC locations during the period of the data breach.

85. Plaintiff and Class or Sub-class members would not have provided their personal information to HBC had they known that HBC would not safeguard their personal information as promised or provide timely notice of a data breach.

86. Plaintiff and Class or Sub-class members fully performed their obligations under the implied contracts with Defendants.

87. Defendants breached the implied contracts by failing to safeguard Plaintiff's and Class or Sub-class members' personal information and failing to provide them with timely and accurate notice when their personal information was compromised in the data breach.

88. The losses and damages Plaintiff and Class or Sub-class members sustained (as described above) were the direct and proximate result of Defendants' breaches of its implied contracts with them.

COUNT V

DECLARATORY JUDGMENT ON BEHALF OF THE CLASS OR SUB-CLASS

89. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

90. Plaintiff and members of the Class or Sub-class entered into an implied contract that required Defendants to provide adequate security for the personal information it collected from their payment card transactions.

91. Defendants owe duties of care to Plaintiff and the members of the Class or, Sub-class that require it to adequately secure personal information.

92. Defendants still possess personal information regarding the Plaintiff and the Class or Sub-class members.

93. Since the data breach, HBC has announced no changes to its data security to fix the vulnerabilities in its systems which permitted the intrusions and to prevent further attacks.

94. Accordingly, HBC and its agents, Saks and Lord & Taylor, still have not satisfied their contractual obligations and legal duties to Plaintiff and the Class or Sub-class. In fact, now that HBC's lax approach towards information security, has become public, the personal information in HBC's possession is more vulnerable than it previously was.

95. Actual harm has arisen in the wake of HBC's data breach and that of its agents, Saks and Lord & Taylor, regarding its contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class or Sub-class. Further, Plaintiff and the members of the Class or Sub-class are at risk of additional or further harm due to the exposure of their personal information and HBC's failure to address the security failings that lead to such exposure.

96. There is no reason to believe that HBC's security measures, and that of its agents, Saks and Lord & Taylor, are any more adequate than they were before the breach to meet HBC's contractual obligations and legal duties, and there is no reason to think HBC or its agents, have no other security vulnerabilities that have not yet been exploited.

97. Plaintiff, therefore, seeks a declaration (1) that HBC's existing security measures, and those of its agents, did not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, HBC and its agents, Saks and Lord & Taylor, must implement and maintain reasonable security measures, including, but not limited to:

a. ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering HBC to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that Defendants segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. ordering that Defendants conduct regular database scanning and securing checks;

g. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps these customers must take to protect themselves.

COUNT VI

VIOLATION OF CONNECTICUT'S UNFAIR TRADE PRACTICES ACT, CONN GEN. STAT. § 42.110a, *ET SEQ.* ON BEHALF OF THE CONNECTICUT SUBCLASS

98. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

99. HBC and its agents are engaged in trade and commerce in Connecticut.

100. HBC and its agents engaged in deceptive, unfair and oppressive acts or practices by failing to disclose and/or misleading Plaintiff and Sub-class members into providing HBC and its agents with the PII, when HBC and its agents knew or were reckless in not knowing that their computer systems were vulnerable to attack by hackers, and in fact were then presently under attack by hackers.

101. Plaintiff and Sub-class members entrusted HBC and its agents with their PII.

102. As alleged herein this Complaint, HBC and its agents engaged in unfair, deceptive, and oppressive acts or practices in the conduct of consumer transactions, including CUPTA, by their:

a. failure to maintain the security of credit and/or debit card account information;

b. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PII;

c. failure to disclose that their computer systems and data security practices were inadequate to safeguard credit and debit card information and other PII from theft;

d. continued acceptance of PII and storage of other personal information after HBC knew or should have known that their systems were being hacked;

e. allowing unauthorized persons to have access to and make unauthorized charges to its customers' credit and/or debit card accounts.

103. HBC and its agents, Saks and Lord & Taylor knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Sub-class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

104. As a direct and proximate result of violation of the CUPTA by HBC and its agents, Plaintiff and Sub-class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Sub-class members; damages arising from their inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for

unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

105. Also as a direct result of HBC's and its agents knowing violation of the CUPTA, Plaintiff and Sub-class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that HBC and its agents engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on HBC's systems on a periodic basis, and ordering HBC to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that HBC and its agents engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that HBC and its agents audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that HBC and its agents segment PII by, among other things, creating firewalls and access controls so that if one area of HBC, Saks or Lord & Taylor is compromised, hackers cannot gain access to other portions of HBC systems;

e. Ordering that HBC, Saks and Lord & Taylor purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that HBC, Saks and Lord & Taylor conduct regular database scanning and securing checks;

g. Ordering that HBC, Saks and Lord & Taylor routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering HBC, Saks and Lord & Taylor to meaningfully educate their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps their customers must take to protect themselves.

106. Plaintiff brings this action on behalf of herself and Class and/or Sub-class members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and Class and Sub-class members and the public from HBC's , Saks' and Lord & Taylor's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. HBC's, Saks' and Lord and Taylor's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class and Sub-class described above, seeks the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class and Sub-class as requested herein, appointing the undersigned as Class or Sub-class counsel, and finding that Plaintiff is a proper representative of the Class and/or Sub-class requested herein;

B. A judgment in favor of Plaintiff and the Class and/or Sub-class awarding them appropriate monetary relief, including actual damages, punitive damages, statutory damages,

equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper.

C. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

D. An order requiring HBC and its agents, Saks and Lord & Taylor, to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

E. A judgment in favor of Plaintiff and the Class or Sub-class awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

F. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: April 20, 2018

Respectfully Submitted,

s/Lynda J. Grant

TheGrantLawFirm, PLLC
521 Fifth Avenue, 17th Floor
New York, NY 10175
t/212-292-4441
f/212-292-4442
lgrant@grantfirm.com

Attorneys for Plaintiffs